AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

LISTING OF CLAIMS:

1 to 8. (Canceled).

9. (Previously Presented) A method for at least one of generating and regenerating an encryption key for a cryptographic method, comprising:

generating a seed S, the seed S being a large random number, only on a side of a user by consulting at least one quantity u known only to the user, the encryption key C and a public key U being generated from the seed S by using at least one predefined deterministic method;

generating a regeneration information R on the side of the user to regenerate the seed S and from which the seed S may be derived deterministically by a trust center by linking only to a secret information v known to the trust center;

storing the regeneration information R so that the regeneration information R is secured against loss,

wherein if the encryption key C is unavailable then the seed S is reconstructable by the trust center by linking the regeneration information to the secret information v.

10. (Currently Amended) The method of claim 9, further comprising providing a key agreement mapping k( ): k(a value x, a value y)=a value z, and wherein:

a) k(k(u,v),w) = k(k(u,w),v) for all u,v,w;

b) from the knowledge of u and k(u,v), v cannot be inferred;

c) from the knowledge of u, k(u,v) and k(u,w), k(k(u,w),v) cannot be inferred;

wherein a public parameter g known to the trust center and a secret key v available at the trust center are linked to a public key V, where V equals [=] k(g,v), of the trust center;

wherein the public key V and the at least one quantity u selected on the user side are linked on the user side to the seed S, where S equals [=] k(V,u);

wherein a key pair made up of an encryption key C and a public user key U is derived from seed S on the user side using the at least one predefined deterministic method; and

wherein to reconstruct the key pair of the encryption key C and the public user key U, the regeneration information R, where R equals [=] k(g,u), is generated on the user side and is stored so as to be protected against loss.

11. (Previously Presented) The method of claim 9, further comprising providing a key agreement mapping k which is a discrete exponential function modulo a large prime number p: $k(x,y) := x^y$ modulo p, and providing that a public parameter g is an element of a mathematical field GF(p) of a high multiplicative power.

12. (Previously Presented) The method of claim 9, further comprising providing a key agreement mapping k which is a multiplication on an elliptic curve.

13. (Currently Amended) The method of claim 9, wherein the trust center calculates the seed S, where S equals [=] $(R,v)_x$ from the regeneration information R so as to reconstruct the encryption key C.

14. (Previously Presented) The method of claim 9, further comprising deriving a new public key U and a new encryption key C when the seed S is calculated, due to loss of at least one of the encryption key C and the public key U; and

verifying by the trust center whether the new public key U is identical to the prior public key U,

wherein when verified that the new public key U is identical to the prior public key U then providing a reconstructed encryption key C to the user.

15. (Previously Presented) The method of claim 10, further comprising providing a plurality of trust centers which employ the key agreement mapping k and the public parameter g;

selecting at least one of the plurality of trust centers, so that each of the selected trust centers assist in generating a partial seed Sv of the seed S being generated on the side of the user and the partial seed Sv being linked on the side of the user to the seed S, in generating the encryption key C;

calculating by the selected trust centers their respective partial seed Sv of the seed S using the regeneration information R, to regenerate the encryption key C in the case of loss;

reconstructing the encryption key C by linking in combination with each other the respective reconstructed partial seed Sv of each respective selected trust center.

16. (Previously Presented) The method of claim 15, wherein the trust center and the plurality of trust centers each use at least one of a respective different function kv and a respective different public parameter gv to create a separate regeneration information Rv for each of the trust centers selected.